AMENDMENTS TO THE CLAIMS

The following is a complete, marked up listing of revised claims with a status identifier in parentheses, underlined text indicating insertions, and strikethrough and/or double-bracketed text indicating deletions.

1. (Previously Presented) An electronic data processing method comprising:

performing, by a security check device, a security check to ascertain a user identity by comparing entered identity information with stored user identity data;

associating the user identity with a user identifier stored in a first data store;

associating the user identifier with at least one user group identifier stored in a second data store;

selecting a user group identifier and acquiring at least one data key associated therewith from a centralized third data store including all available keys, wherein the at least one user group identifier and the at least one data key are associated with one another; and

performing, by at least one processor, at least one of encrypting and decrypting data using the acquired at least one data key and inhibiting user recognition of the acquired at least one data key; wherein

the data are medically relevant,

users include personnel within a medical facility, and

common user group identifiers are assigned the same data key.

2. (Previously Presented) The method as claimed in claim 1, wherein the security check involves at least one of checking a user-specific biometric data, an electronic key and a mechanical key.

3. – 4. (Canceled)

5. (Previously Presented) The system as claimed in claim 8, wherein the at least one data key is accessible using a data telecommunication device.

6. (Previously Presented) The method as claimed in claim 1, wherein a plurality of data keys are simultaneously assignable to one user identifier.

7. (Canceled).

8. (Currently Amended) An electronic data processing system comprising:

a security check device to ascertain user identity stored at a first data store and to retrieve at least one user identifier and associated user identity data;

a second data store for storage and retrieval of the at least one user identifier and associated at least one user group identifier;

a centralized third data store for storage and retrieval of all available data keys, the centralized third data store including at least one associated user group identifier matched with at least one associated data key; and

at least one processor to ascertain a user identifier by comparing data ~~between~~ of the security check device and the first data store, to ascertain at least one user group from the second data store, to ascertain at least one

data key for at least one user group from the third data store, and for performing at least one of encrypting and decrypting data using the at least one data key; wherein

the data are medically relevant,

users include personnel within a medical facility, and

common user group identifiers are assigned the same data key.

9. (Previously Presented) The electronic data processing system as claimed in claim 8, wherein the security check device reads biometric data from a user.

10. (Currently Amended) The electronic data processing system as claimed in claim 8, wherein the security check device uses ~~users~~ at least one of an electronic and mechanical key, which are user-specific.

11. (Canceled).

12. (Original) The electronic data processing system as claimed in claim 8, wherein the system uses a data telecommunication device to access the third data store.

13. (Original) The electronic data processing system as claimed in claim 8, wherein the system is a medical workstation for handling medically relevant data.

14. (Previously Presented) A computer-readable storage medium including computer executable instructions that, when executed, cause a computer to carry out the method as claimed in claim 1.

15. - 21. (Canceled).

22. (Previously Presented) A method for at least one of encryption and decryption of data, comprising:

performing, by a security check device, a security check to ascertain user identity by comparing entered identity information with stored user identity data;

associating the user identity with a user identifier stored in a first data store;

associating the user identifier with a user group including a plurality of users such that a data key for at least one of encrypting and decrypting data is assigned to the user based on the group with which the user identifier is associated, the same data key being assignable to the plurality of users; and

at least one of encrypting or decrypting data, by at least one processor, using the assigned data key; wherein

the data are medically relevant,

the plurality of users include personnel within a medical facility, and

common user group identifiers are assigned the same data key.

23. (Previously Presented) A computer-readable storage medium including computer executable instructions that, when executed, cause a computer to, carry out the method as claimed in claim 22.

24. (Previously Presented) The method as claimed in claim 22, wherein the security check involves checking biometric data of a user.

25. (Previously Presented) The method as claimed in claim 22, wherein the security check involves checking at least one of an electronic and mechanical key, which are user-specific.

26. (Previously Presented) The method as claimed in claim 22, wherein the data key is ascertained by comparing the user identity data obtained in the security check with content of a data key memory.

27. (Original) The method as claimed in claim 26, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

28. (Original) The method as claimed in claim 22, wherein a plurality of data keys are simultaneously assignable to one user.

29. (Canceled).

30. (Original) The method of claim 22, wherein users associated with a common user group are assigned the same data key.

31. (Canceled).

32. (Previously Presented) The method of claim 1, wherein a user identifier associated with a common user group identifier is assigned the same data key.

33. (Previously Presented) The system of claim 8, further comprising:
a fourth data store for storage and retrieval of encrypted data.

34. (Original) The system of claim 8, wherein at least one of the first data store, the second data store and the fourth data store are combined.

35. (Previously Presented) The system of claim 8, wherein the first data store comprises:
mechanical memory, electronic memory, and magnetic and optical media data storage.

36. (Original) The system of claim 8, wherein the third data store is isolated from the first, second and fourth data stores.

37. (Original) The system of claim 8, wherein data entry and retrieval is at least one of manual and automated.

38. (Original) The system of claim 12, wherein the data telecommunications device is removably and operatively associated with a computer network for transfer of data.

39. (Previously Presented) The system of claim 8, wherein the at least one processor accesses the centralized third data store through a channel via one of an access and restriction process.

40. (Original) The system of claim 39, wherein the channel access and restriction process functions operatively with the security check device.